INFORMATION AND CONTROL 15, 67–69 (1969)

Primitive Trinomials Whose Degree is a Mersenne Exponent

NEAL ZIERLER

Institute for Defense Analyses, Princeton, New Jersey

We list all irreducible trinomials over GF(2) of every degree p for which $2^p - 1$ is known to be prime, and describe briefly the method used to find them.

Let p and k be integers such that $p > k > 0$ and $2^p - 1$ is prime. Suppose the trinomial $T_{p,k}(x) = x^p + x^k + 1$ is irreducible over $GF(2)$. Then it is automatically primitive (that is, has generators of the multiplicative group of $GF(2^p)$ as roots) since the order of a root of a polynomial of degree n over $GF(2)$ divides $2^n - 1$. It is the purpose of this note to list all irreducible trinomials over $GF(2)$ of every degree p for which $2^p - 1$ is known to be prime. This completes a task to which a number of authors have contributed. Among these we mention Gillies (1964) who lists the 23 known primes of this type, including three new ones; Watson (1962), irreducible polynomials of degree less than 100; Zierler and Brillhart (1968), all irreducible trinomials of degree $n \leqq 1000$ with periods for some for which the factorization of $2^n - 1$ is known (the completion to appear soon); Rodemich and Rumsey (1968) who list all irreducible trinomials of degrees 127, 521, 607, 1279, 2203, and 2281.

The computation was done on a CDC 6600; about 95% of the running time was spent on the six new cases: $p > 2281$. The first of three tests is based on results of Swan (1962): if $p \equiv \pm 3$ modulo 8, only $k = 2$ need be considered, for in this case, $1 \leqq k < p/2$, $k \neq 2$ implies that $x^p + x^k + 1$ has an even number of irreducible factors, and so is composite. It turns out that $x^p + x^2 + 1$ is composite for those 8 of the 23 primes which are >5 and congruent to ± 3 modulo 8, so there are no irreducibles of these degrees. In case $p \equiv \pm 1$ modulo 8, however, Swan's results eliminate only the case $k = 2$ and, indeed, the 12 primes congruent to ± 1 modulo 8 all have irreducible trinomials.

The second test is based on the observation that $x^p + x^k + 1$ has an

irreducible factor of degree n if and only if the trinomial obtained when p and k are reduced modulo $2^n - 1$ does, since every irreducible polynomial over $GF(2)$ of degree n divides $x^{2^n-1} - 1$. The test consisted in performing this reduction for $n = 3, \cdots, 10$ and, when both residues were less than 60, looking in a table of complete factorizations of all trinomials of degree less than 60 to see if this trinomial had an irreducible factor of degree n. Incidentally, it took only about a minute to generate the table, using a program based on ideas of A. M. Gleason.[1] Approximately 70% of all trinomials considered were eliminated by this test.

If $f(x) = x^p + x^k + 1$ survived the tests described above, we computed x^{2^p} modulo f, since $x^{2^p} \equiv x$ modulo f if and only if every irreducible factor of f has degree dividing p, hence equal to p; that is, if and only if f is irreducible. Because of the large number of operations involved, it was important to make this procedure reasonably efficient, and this was accomplished as follows. First, squaring to obtain x^{2^n} given $x^{2^{n-1}}$ modulo f was done not by multiplication but by inserting zeros between the bits of $x^{2^{n-1}}$, since $(\sum a_i x^i)^2 = \sum a_i x^{2i}$ over $GF(2)$. This, of course, produces a polynomial of degree around $2p - 2$ from one of degree around $p - 1$. Second, advantage is taken in reducing modulo f of the fact that f is a trinomial with second exponent less than half the degree. Let $g(x)$ be the squared polynomial. Except for the first few steps, it is of degree $2p - 2$ or a little less. First we add the part of g of degree greater than $p - 1$, multiplied by x^{-p}, to g. Second, we add the part of g of degree greater than $p - 1$, multiplied by x^{k-p}, to the part of g of degree less than p, and replace the part of g of degree greater than $p - 1$ with the terms of $x^{k-p}g$ of degree greater than $p - 1$. We now have a polynomial of degree less than $p + k$. We repeat with it the process just described, completing the reduction of x^{2^n} modulo f.

In the table which follows, the entries under k are all numbers less than $p/2$ for which the trinomial $x^p + x^k + 1$ is irreducible.

p	k
2	1
3	1
5	2
7	1, 3
13	NONE

[1] Unpublished but see Berlekamp (1968), Ch. 6 for another effective method.

17	3, 5, 6
19	NONE
31	3, 6, 7, 13
61	NONE
89	38
107	NONE
127	1, 7, 15, 30, 63
521	32, 48, 158, 168
607	105, 147, 273
1279	216, 418
2203	NONE
2281	715, 915, 1029
3217	67, 576
4253	NONE
4423	271, 369, 370, 649, 1393, 1419, 2098
9689	84, 471, 1836, 2444, 4187
9941	NONE
11213	NONE

RECEIVED: May 23, 1969

REFERENCES

BERLEKAMP, E. R. (1968), "Algrbraic coding theory." McGraw-Hill, New York.

GILLIES, D. B. (1964), Three new Mersenne primes and a Statistical theory. *Math. Comp.* **18**, 93–95.

RODEMICH, E. R. AND RUMSEY, H., JR. (1968), Primitive trinomials of high degree. *Math. Comp.* **22**, 863–865.

SWAN, R. G. (1962), Factorization of polynomials over finite fields. *Pac. J. Math.* **12**, 1099–1106.

WATSON, E. J., (1962), Primitive polynomials (mod 2). *Math. Comp.* **16**, 368–369.

ZIERLER, N. AND BRILLHART, J. (1968), On primitive trinomials (mod 2). *Inform. Control* **13**, 541–554.